



February 21, 2014

Marlene H. Dortch, Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12th Street S. W., Suite TW-A325  
Washington, D.C. 20554

**RE: EB Docket 06-36 - Certification of CPNI Filing, for Westlink Communications, LLC**

On behalf of Westlink Communications, LLC ("Westlink"), and pursuant to Section 64.2009(e) of the FCC rules, please find attached the carrier's 2013 CPNI certification with accompanying statement. Pursuant to FCC approval, Westlink underwent a Transfer of Control in August 2013, and these documents are submitted by the new management to certify compliance with the FCC rules during its time of operation. The previous owner will submit a certification for Westlink for its period of operation.

Please feel free to contact me with any question or requests for additional information.

Sincerely,

/s/

Stacey Brigham  
Senior Regulatory Consultant

Cc: Best Copy and Printing, Inc., 445 12th Street, Suite CY-B402, Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

1. Date filed: February 5, 2014
2. Name of company(s) covered by this certification: WestLink Communications, LLC
3. Form 499 Filer ID: 821344
4. Name of signatory: Craig Mock
5. Title of signatory: General Manager
6. Certification:

I, Craig Mock, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

It is my understanding that prior to the current owner's operation period, which began in August 2013, the company received one anonymous customer complaint in the past year concerning the unauthorized release of CPNI by an employee to an unauthorized person. As the Company had no information as to the alleged complainant, employee or victim, the Company could not determine whether a breach had occurred.

The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed  \_\_\_\_\_, as agent of the carrier

**Attachments:** Accompanying Statement explaining CPNI procedures

## **CPNI Usage Policy Statement**

Pursuant to Section 64.2009(e) of the Federal Communications Commission's ("FCC") rules, this statement explains how WestLink Communications, LLC's (the "Company") operating procedures ensure compliance with Part 64, Subpart U of the FCC's rules.

### **Company CPNI Policies**

Company has established operating procedures that ensure compliance with the FCC's regulations regarding the protection of customer proprietary network information (CPNI).

Company has adopted a manual and keeps it up updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.

Company continually educates and trains its employees regarding the appropriate use of CPNI. Company provides annual training for all employees and individual training for new employees. Employees are provided with a continually updated Code of Ethics that includes the FCC's regulations regarding the protection of CPNI. Company has established disciplinary procedures should an employee violate the CPNI procedures established by Company. These disciplinary procedures can include termination of employment.

Company has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.

Company maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Company also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.

Company has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Company's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

Company has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Company's retail locations, electronically or otherwise. In connection with these procedures, Company has established a system of personal identification numbers (PINs), passwords and back-up authentication methods for all customer and accounts, in compliance with the requirements of the applicable FCC rules.

Company has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.

Company has established procedures to notify law enforcement of unauthorized disclosure of CPNI. In the event of a CPNI breach, Company complies with the FCC's rules regarding notice to law enforcement and customers. Company maintains records of any discovered breaches and notifications to the United States Secret Service (USSS) and FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two year.

#### **Actions Taken Against Data Brokers and Customer Complaints**

Company has taken no actions against data brokers in the last year. The company received one anonymous customer complaint in the past year concerning the unauthorized release of CPNI by an employee to an unauthorized person. As the Company had no information as to the alleged complainant, employee or victim, the Company could not determine whether a breach had occurred.